Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method for access control of a hardfile in a computer system having an operating system, the method comprising:

detecting a special boot condition during a pre-boot test of the computer system, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system; and

in response to detecting the special boot condition, adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile, the size of the partition of the hardfile being adjusted to reduce access of the operating system to data stored on the hardfile during the hardware tamper or the software tamper.

2. (Previously Presented) The method of claim 1, wherein adjusting a size of a partition of the hardfile dynamically sets a maximum accessible size of the hardfile.

3. (Previously Presented) The method of claim 1, wherein the hardfile is a hard drive.

4. (Previously Presented) The method of claim 1, wherein the operating system is stored on a first part of the hardfile and user data is stored on a second part of the hardfile, and wherein adjusting a size of a partition of the hardfile sets the hardfile access to exclude the second part of the hardfile from access by the operating system.

5. (Previously Presented) The method of claim 2, wherein the operating system is stored on a first part of the hardfile and user data is stored on a second part of the hardfile, and wherein adjusting a size of a partition of the hardfile sets the hardfile maximum size to exclude the second part of the hardfile from access by the operating system.

6. (Currently Amended) The method of claim 4, wherein:

the ~~special boot condition is a~~ hardware tamper ~~detect~~ corresponds to installation of new hardware for use with the computer system; and

the software tamper corresponds to installation of a new software application on the computer system.

7-12. (Cancelled)

13. (Currently Amended) A storage system for a computer system having an operating system and a pre-boot procedure, the storage system comprising:

a hardfile for non-volatile storage of the operating system on a first part of the hardfile and a plurality of user data on a second part of the hardfile; and

a hardfile controller, coupled to the hardfile and responsive to a special boot condition detected by the pre-boot procedure, operable to dynamically reconfigure operating system access to the hardfile including adjusting a size of a partition of the hardfile to permit access to both the first part of the hardfile and the second part of the hardfile in a first mode and to permit access to only the first part of the hardfile in a second mode, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system.

14. (Currently Amended) A storage system for a computer system having an operating system, the storage system comprising:

a hardfile for non-volatile storage of the operating system on a first part of the hardfile and a plurality of user data on a second part of the hardfile; and

a hardfile controller, coupled to the hardfile and responsive to a special boot condition detected by a pre-boot procedure of the computer system, operable to dynamically reconfigure operating system access to the hardfile including adjusting a size of a partition of the hardfile to permit access to both the first part of the hardfile and the second part of the hardfile in a first mode and to permit access to only the first part of the hardfile in a second mode, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system.

15. (Currently Amended) A storage system controller for a hardfile of a computer system having an operating system and a pre-boot procedure, the hardfile for non-volatile storage of the operating system on a first part of the hardfile and a plurality of user data on a second part of the hardfile, the storage system controller comprising:

a hardfile controller, coupled to the hardfile and responsive to a special boot condition detected by the pre-boot procedure, operable to dynamically reconfigure operating system access to the hardfile including adjusting a size of a partition of the hardfile to permit access to both the first part of the hardfile and the second part of the hardfile in a first mode and to permit access by the operating system to only the first part of the hardfile in a second mode, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system.

16. (Currently Amended) A storage system controller for a hardfile of a computer system having an operating system, the hardfile for non-volatile storage of the operating system on a first part of the hardfile and a plurality of user data on a second part of the hardfile, the storage system controller comprising:

a hardfile controller, coupled to the hardfile and responsive to a special boot condition detected by a pre-boot procedure of the computer system, operable to dynamically reconfigure operating system access to the hardfile including adjusting a size of a partition of the hardfile to permit access to both the first part of the hardfile and the second part of the hardfile in a first mode and to permit access by the operating system to only the first part of the hardfile in a second mode, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system.

17. (Currently Amended) A hardfile system for a computer system, the hardfile system comprising:

a hardfile for non-volatile storage of a operating system and user data;

means, coupled to the computer system, for detecting a special boot condition during a pre-boot test of the computer system, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system; and

means, coupled to the hardfile and to the detecting means, for adjusting a size of a partition of the hardfile to alter an operating system access configuration of the hardfile in response to detecting the special boot condition, the size of the partition of the hardfile being adjusted to reduce access of the operating system to data stored on the hardfile during the hardware tamper or the software tamper.

18. (Cancelled)

19. (Currently Amended) A computer usable medium having computer readable program code means embodied therein for access control of a hardfile, responsive to a hardfile controller included in a computer system having an operating system performing a pre-boot test, the computer readable program code means in the computer usable medium comprising:

computer readable program code means for causing the computer system to detect a special boot condition during the pre-boot test, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system; and

computer readable program code means for causing the computer system to adjust a size of a partition of the hardfile to alter an operating system access configuration parameter of the hardfile in response to detection of the special boot condition, the size of the partition of the hardfile being adjusted to reduce access of the operating system to data stored on the hardfile during the hardware tamper or the software tamper.

20. (Currently Amended) The computer usable medium of claim 19, wherein:

the ~~special boot condition is a~~ hardware tamper ~~detect~~ corresponds to installation of new hardware for use with the computer system ; and

the software tamper corresponds to installation of a new software application on the computer system.

21. (Original) The computer usable medium of claim 19, wherein the hardfile is a hard disk.

22. (Original) The computer usable medium of claim 21, wherein the configuration parameter is a SETMAX value.

23. (Currently Amended) A computer readable medium containing program instructions, tangibly stored thereon, for access control of a hard file in a computer system, the program instructions for:

detecting a special boot condition during the pre-boot test, the special boot condition being a detect of a hardware tamper of the computer system or a detect of a software tamper of the computer system; and

in response to detecting the special boot condition, adjusting a size of a partition of the hardfile to alter an operating system access configuration of an access parameter of the hardfile, the size of the partition of the hardfile being adjusted to reduce access of the operating system to data stored on the hardfile during the hardware tamper or the software tamper.

24. (Currently Amended) The computer readable medium of claim 23, wherein:

the ~~special boot condition is a~~ hardware tamper ~~detect~~ corresponds to installation of new hardware for use with the computer system; and

the software tamper corresponds to installation of a new software application on the computer system.

25. (Original) The computer readable medium of claim 23, wherein the hardfile is a hard disk.

26. (Previously Presented) The method of claim 1, wherein adjusting a size of a partition of the hardfile includes adjusting a size of a Protected Area Run Time Interface Extension Services

(PARTIES) partition.

27. (Previously Presented) The method of claim 26, further comprising using a SETMAX procedure to adjust the size of the PARTIES partition.

28. (Currently Amended) A method for controlling access of an operating system to data in a hard drive of a computer system, the method comprising:

providing a computer system including a hard drive, the hard drive including one or more of user data or software applications in a first portion of the hard drive;

initiating a power on self-test of the computer system;

determining whether a pre-determined condition occurs to limit access to the one or more of user data or software applications in the first portion of the hard drive, the pre-determined condition being one or more of

a detection of installation of a new hardware for use with the computer system, or

a detection of installation of a new software application on the computer system;

and

if the pre-determined condition occurs then dynamically adjusting a size of a partition of the hard drive during the power on self-test to exclude access of the operating system to the one or more of user data or software applications in the first portion of the hard drive during the installation of the new hardware for use with the computer system or the installation of the new software application on the computer system;

otherwise providing the operating system full access to the one or more of user data or software applications in the first portion of the hard drive.

29. (Previously Presented) The method of claim 28, wherein dynamically adjusting a size of a partition includes adjusting a size of a Protected Area Run Time Interface Extension Services (PARTIES) partition.

30. (Previously Presented) The method of claim 29, wherein the hard drive is a ATAPI-4 compliant hard drive.

31. (New) The method of claim 28, wherein dynamically adjusting a size of a partition of the hard drive further comprises providing the operating system access to a diagnostic tool on the hard drive to permit one or more of the installation of the new hardware for use with the computer system, or the installation of the new software application on the computer system.